Upgrading or Downgrading the Cisco Nexus 9000 Series NX-OS Software

This chapter describes how to upgrade or downgrade the Cisco NX-OS software. It contains the following sections:

About the Software Image

Each device is shipped with the Cisco NX-OS software preinstalled. The Cisco NX-OS software consists of one NX-OS software image. Only this image is required to load the Cisco NX-OS operating system.

In Cisco NX-OS Release 10.1(1), 10.1(2), and 10.2(1)F there are 32 and 64 bit images.

- The 32-bit Cisco NX-OS image file has the image filename that begins with "nxos" (for example, nxos.10.1.1.bin).
- The 64-bit Cisco NX-OS image file has the image filename that begins with "nxos64" (for example, nxos64.10.1.1.bin).

Note Beginning with Cisco NX-OS Release 10.1(x), only 9300-GX platforms support 64-bit image. Beginning with Cisco NX-OS Release 10.2(1)F, all platforms support 64-bit image.

Beginning with Cisco NX-OS Release 10.2(2)F all Cisco Nexus platforms are operating only on 64-bit images and there are two 64-bit images.

- The 64-bit Cisco NX-OS image file has the image filename that begins with "nxos64-cs" (for example, nxos64-cs.10.2.2.F.bin) : This image is supported on Cisco Nexus 9000 -EX, -FX, -FX2, -FXP, -FX3, -GX, -GX2, and 9364C series fixed switches and Nexus 9000 series modular switches
- The 64-bit Cisco NX-OS image file has the image filename that begins with "nxos64-msll" (for example, nxos64-msll.10.2.2.F.bin) This image is supported on Cisco Nexus 9000 -R and -R2 series modular switches, Cisco Nexus 3600 series fixed switches and Cisco Nexus 3500-XL switches.

For 32-bit or 64-bit image support on respective platforms, see the relevant version of the Cisco Nexus 9000 Series Release Notes on Cisco.com.

The Cisco Nexus 9000 Series switches support disruptive software upgrades and downgrades by default.

Note Another type of binary file is the software maintenance upgrade (SMU) package file. SMUs contain fixes for specific defects. They are created to respond to immediate issues and do not include new features. SMU package files are available for download from Cisco.com and generally include the ID number of the resolved defect in the filename (for example, n9000-dk10.1.1.**CSCab00001**.gbin). For more information on SMUs, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*.

Note Cisco also provides electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known hardware issues. The EPLD image upgrades are independent from the Cisco NX-OS software upgrades. For more information on EPLD images and the upgrade process, see the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes.

About ISSU

An in-service software upgrade (ISSU) allows you to upgrade the device software while the switch continues to forward traffic. ISSU reduces or eliminates the downtime typically caused by software upgrades. You can perform an ISSU, also known as a non-disruptive upgrade, for some switches. (See the ISSU Platform Support, on page 16 for a complete list of supported platforms.)

The default upgrade process is disruptive. Therefore, ISSU needs to be enabled using the command-line interface (CLI), as described in the configuration section of this document. Using the non-disruptive option helps ensure a non-disruptive upgrade. The guest shell is disabled during the ISSU process and it is later reactivated after the upgrade.

Enhanced ISSUs are supported for some Cisco Nexus 9000 Series switches.

The following ISSU scenarios are supported:

- Performing standard ISSU on Top-of-Rack (ToR) switches with a single supervisor
- Performing enhanced ISSU on Top-of-Rack (ToR) switches with a single supervisor

Performing Standard ISSU on Top-of-Rack (ToR) Switches with a Single Supervisor

The ToR Cisco Nexus 9300 platform switches are the NX-OS switches with single supervisors. Performing ISSU on the Cisco Nexus 9000 Series switches causes the supervisor CPU to reset and to load the new software version. After the CPU loads the updated version of the Cisco NX-OS software, the system restores the control plane to the previous known configuration and the runtime state and it gets in-sync with the data plane, thereby completing the ISSU process.

The data plane traffic is not disrupted during the ISSU process. In other words, the data plane forwards the packets while the control plane is being upgraded, any servers that are connected to the Cisco Nexus 9000 Series switches do not see any traffic disruption. The control plane downtime during the ISSU process is approximately less than 120 seconds.

Performing Enhanced ISSU on Top-of-Rack (ToR) Switches with a Single Supervisor

Note Enhanced ISSU may not be supported if there are any underlying kernel differences. The system will prompt the following message:

```
Host kernel is not compatible with target image. Full ISSU will be performed and control
plane will be impacted.
```

In effect, system will perform non-disruptive ISSU instead of enhanced ISSU.

The Cisco NX-OS software normally runs directly on the hardware. However, configuring enhanced or container-based ISSU on single supervisor ToRs is accomplished by creating virtual instances of the supervisor modules and the line cards. With enhanced ISSU, the software runs inside a separate Linux container (LXC) for the supervisors and the line cards. A third container is created as part of the ISSU procedure, and it is brought up as a standby supervisor.

The virtual instances (or the Linux containers) communicate with each other using an emulated Ethernet connection. In the normal state, only two Linux containers are instantiated: vSup1 (a virtual SUP container in an active role) and vLC (a virtual linecard container). Enhanced ISSU requires 16G memory on the switch.

To enable booting in the enhanced ISSU (LXC) mode, use the **[no] boot mode lxc** command. This command is executed in the config mode. See the following sample configuration for more information:

```
switch(config)# boot mode lxc
Using LXC boot mode
Please save the configuration and reload system to switch into the LXC mode.
switch(config)# copy r s
[########################################] 100%
Copy complete.
```

Note When you are enabling enhanced ISSU for the first time, you have to reload the switch first.

During the software upgrade with enhanced ISSU, the supervisor control plane stays up with minimal switchover downtime disruption and the forwarding state of the network is maintained accurately during the upgrade. The supervisor is upgraded first and the line card is upgraded next.

The data plane traffic is not disrupted during the ISSU process. The control plane downtime is less than 6 seconds.

Note In-service software downgrades (ISSDs), also known as non-disruptive downgrades, are not supported.

For information on ISSU and high availability, see the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide.

Recommendations for Upgrading the Cisco NX-OS Software

Cisco recommends performing a Nexus Health and Configuration Check before performing an upgrade. The benefits include identification of potential issues, susceptible Field Notices and Security Vulnerabilities, missing recommended configurations and so on. For more information about the procedure, see Perform Nexus Health and Configuration Check.

Prerequisites for Upgrading the Cisco NX-OS Software

Upgrading the Cisco NX-OS software has the following prerequisites:

- For ISSU compatibility for all releases, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.
- Ensure that everyone who has access to the device or the network is not configuring the device or the network during this time. You cannot configure a device during an upgrade. Use the **show configuration session summary** command to verify that you have no active configuration sessions.
- Save, commit, or discard any active configuration sessions before upgrading or downgrading the Cisco NX-OS software image on your device. On a device with dual supervisors, the active supervisor module cannot switch over to the standby supervisor module during the Cisco NX-OS software upgrade if you have an active configuration session.
- To transfer NX-OS software images to the Nexus switch through a file transfer protocol (such as TFTP, FTP, SFTP, SCP, etc.), verify that the Nexus switch can connect to the remote file server where the NX-OS software images are stored. If you do not have a router to route traffic between subnets, ensure that the Nexus switch and the remote file server are on the same subnetwork. To verify connectivity to the remote server, transfer a test file using a file transfer protocol of your choice or use the ping command if the remote file server is configured to respond to ICMP Echo Request packets. An example of using the **ping** command to verify connectivity to a remote file server 192.0.2.100 is shown below:

```
switch# ping 192.0.2.100 vrf management
PING 192.0.2.100 (192.0.2.100): 56 data bytes
64 bytes from 192.0.2.100: icmp_seq=0 ttl=239 time=106.647 ms
64 bytes from 192.0.2.100: icmp_seq=1 ttl=239 time=76.807 ms
64 bytes from 192.0.2.100: icmp_seq=2 ttl=239 time=76.593 ms
64 bytes from 192.0.2.100: icmp_seq=3 ttl=239 time=81.679 ms
64 bytes from 192.0.2.100: icmp_seq=4 ttl=239 time=76.5 ms

--- 192.0.2.100 ping statistics ---
```

```
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 76.5/83.645/106.647 ms
```

- For non-disruptive ISSU in spanning tree topology, before running the **show spanning-tree issu-impact** command, verify the following criteria:
  - No Topology change must be active in any STP instance
  - Bridge assurance(BA) should not be active on any port (except MCT and vPC peer link)
  - There should not be any Non-Edge Designated Forwarding port (except MCT and vPC peer link)
  - ISSU criteria must be met on the vPC peer switch

For more information on configuration sessions, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide* specific to your release.

Prerequisites for Downgrading the Cisco NX-OS Software

Downgrading the Cisco NX-OS software has the following prerequisites:

- Before you downgrade from a Cisco NX-OS release that supports the Control Plane Policing (CoPP) feature to an earlier Cisco NX-OS release that does not support the CoPP feature, you should verify compatibility using the **show incompatibility nxos bootflash:***filename* command. If an incompatibility exists, disable any features that are incompatible with the downgrade image before downgrading the software.

Cisco NX-OS Software Upgrade Guidelines

Before attempting to upgrade to any software image, follow these guidelines:

- For a device that is running on Cisco Nexus Release 10.1(2), 10.2(1)F, and 10.2(2)F, ND-ISSU is not supported if L2 sub-interfaces are configured.
- Beginning with Cisco NX-OS Release 10.2(2)F, Cisco Nexus 9504 and 9508 platform switches, and Cisco Nexus 9508-R, R2, and RX line cards support Cisco NX-OS 64-bit images. Disruptive upgrade from earlier releases to 10.2(2)F 64-bit NX-OS image is supported. Cisco NX-OS 32-bit image is not supported on these platform switches anymore.
- Beginning with Cisco NX-OS Release 10.2(2)F, FCoE/FC NPV is supported on N9K-C9336C-FX2-E platform switches.

  ISSU with with FCoE (Fiber Channel over Ethernet)/FC (Fiber Channel) NPV (N-port Virtualization) is supported on some Cisco Nexus 9000 switches. An ISSU allows you to upgrade the device software while the switch continues to forward traffic. You can perform an in-service software upgrade (ISSU), also known as a nondisruptive upgrade, for some Cisco Nexus 9000 switches. The default upgrade process is disruptive. Using the nondisruptive option helps ensure a nondisruptive upgrade.

  Fibre Channel N-port Virtualization (NPV) can co-exist with VXLAN on different fabric uplinks but on same or different front panel ports on the Cisco Nexus 93180YC-FX, N9K-C9336C-FX2-E, and N9k-C93360YC-FX2 switches.

- Beginning with Cisco NX-OS Release 10.2(2)F, ND ISSU is supported for FEX and you need to re-adjust the BGP **graceful-restart restart time** command for the upgrade to work non-disruptively. This must be done for each FEX upgrade one-by-one.

  The following example shows the time taken to re-adjust bgp-graceful restart-time for each non-disruptive FEX upgrade.

```
In the Non-disruptive upgrade with FEX, each FEX will upgrade taking about 90 secondss

(1.5 minutess) sequentially (one-by-one and not a parallel upgrade).
  Total non-disruptive upgrade time for all FEX = No. of fex * time taken per fex
                                     For 10 FEX = 10 * 90
                                                = 900 seconds or 15 minutes
```

- MPLS strip, GRE strip, and any underlying ACL configuration is not ISSU compatible when you perform ND ISSU to Cisco NX-OS Release 10.2(2)F from a previous release.

  After ND ISSU to Cisco NX-OS Release 10.2(2)F or 10.2(3)F from a previous release, post GRE strip dot1q tunnel VLAN_tag might be missing. Workaround for this issue is to remove and add port ACL from L2 interfaces for GRE strip enabled interface.

- For ISSU compatibility for all releases, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

- Beginning from Cisco NX-OS Release 10.2(1), Cisco Nexus 9300 and 9500 platform switches support 64-bit image.

- Non-disruptive upgrade to 64-bit image is supported from Cisco NX-OS Release 9.3(9) onwards. See supported platforms in Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

- Beginning from Cisco NX-OS Release 10.2(8)M onwards, Cisco Nexus 9300-FX3 supports non-disruptive upgrade.

- Beginning with Cisco NX-OS Release 10.1(1), during the disruptive upgrade to the 64-bit image or a downgrade from 64-bit to 32-bit image, if feature ITD is enabled, refer to *Guidelines and Limitations for ITD* in the *Cisco Nexus 9000 Series NX-OS Intelligent Traffic Director Configuration Guide, Release 10.1(x)*, if the upgrade or downgrade proceeds with an ASIC reload.

- Beginning with Cisco NX-OS Release 10.1(x), when an existing SMU is active, if you install a bundle that contains the existing active SMU, the installer installs only the non-existing SMUs.

- When you use **install all** with **no-reload** option, the saved configuration cannot be used before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with new version of NX-OS.

- For switches that are in LXC boot mode, when upgrading image from Cisco NX-OS Release 10.1(1) or earlier releases to Cisco NX-OS Release 10.2(x), the upgrade will be disruptive.

- While upgrading from NX-OS releases prior to 10.2(2)F to 10.2(2)F or later releases, configure the **mode tap-aggregation** command before attaching TapAgg ACLs on Layer 2 interface.

- Beginning with Cisco NX-OS Release 10.2(3)F, for switches that are in LXC mode and for non-destruptive upgrade, a new option **skip-kernel-upgrade** is added to **install** command.

- The following are the two methods by which the ND ISSU can be performed in LXC mode:

  - ND ISSU in LXC mode - Switchover-based ISSU that is similar to EOR. Second SUP is brought up in new container and switchover is done. The second SUP now becomes the new active. There is no change to the kernel.

  - Fallback ND LXC ISSU - This is only done when the above switchover-based ISSU cannot be done (SRG Kernel incompatible or less memory). The kernel is upgraded.
  - skip-kernel-upgrade option will force ND ISSU in LXC mode - Switchover-based ISSU (even in case when running) and target kernels are incompatible.

- When upgrading from Cisco NX-OS Release 9.3(3) to Cisco NX-OS Release 9.3(6) or later, if you do not retain configurations of the TRM enabled VRFs from Cisco NX-OS Release 9.3(3), or if you create new VRFs after the upgrade, the auto-generation of **ip multicast multipath s-g-hash next-hop-based** CLI, when feature **ngmvpn** is enabled, will not happen. You must enable the CLI manually for each TRM enabled VRF. For the configuration instructions, see the *Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, Release 10.1(x)*.
- When you upgrade a Cisco Nexus 9000 device to Cisco NX-OS Release 10.1(x), if a QSFP port is configured with the manual breakout command and is using a QSA, the configuration of the interface Ethernet 1/50/1 is no longer supported and must be removed. To restore the configuration, you must manually configure the interface Ethernet 1/50 on the device.
- When redistributing static routes, Cisco NX-OS requires the **default-information originate** command to successfully redistribute the default static route starting in 7.0(3)I7(6).
- To perform an EPLD upgrade after an ISSU upgrade from Cisco NX-OS Release 7.x to Cisco NX-OS Release 9.3(x), before starting the EPLD upgrade, add the copy run start command.
- When upgrading from Cisco NX-OS Release 9.2(4) or earlier releases to Cisco NX-OS Release 9.3(4) or later, running configuration contains extra TCAM configuration lines. You can ignore these extra lines as they do not have an effect on the upgrade and configuration.
- When performing an ISSU from Cisco NX-OS Release 9.3(1) or 9.3(2) to Cisco NX-OS Release 9.3(3) or later, ensure that the features with user-defined ports, such as **<ssh port>**, are within the prescribed port range. If the port range is incorrect, follow the syslog message recommendation. For more information about the port range, see Cisco Nexus 9000 Series NX-OS IP SLAs Configuration Guide, Release 10.1(x).
- When upgrading from Cisco NX-OS Release 9.2(2) or earlier releases to Cisco NX-OS Release 10.1(x), you need to make sure that ingress RACL TCAM region is not more than 50% full. Otherwise, the atomic update feature will be enabled after the upgrade and interfaces with RACLs that exceed 50% of TCAM allocation will remain down.
- Beginning with Cisco NX-OS Release 10.1(1), ISSU is supported on FC/FCoE switch mode on Cisco Nexus 93360YC-FX2. For more information about the FC/FCoE switch mode and supported hardware, see *Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 10.1(x)*.
- Beginning with Cisco NX-OS Release 10.1(1), Enhanced ISSU is supported on FC/FCoE switch mode for Cisco Nexus 93180YC-FX and 93360YC-FX2 switches. For more information about the FC/FCoE switch mode and supported hardware, see *Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 10.1(x)*.
- Beginning with Cisco NX-OS Release 10.1(1), Enhanced ISSU is supported on FC/FCoE NPV mode for Cisco Nexus 93180YC-FX and 93360YC-FX2 switches. For more information about the FC/FCoE NPV mode and supported hardware, see *Cisco Nexus 9000 Series NX-OS FC-NPV and FCoE NPV Configuration Guide, Release 10.1(x)*.
- Software image compaction is only supported on Cisco Nexus 9300-series platform switches.

- The compressed image of Cisco Nexus 3000-series is hardware dependent and can only be used on the same device that it got compressed or downloaded from CCO. Do not use the Nexus 3000-series compressed image on Nexus 9000-series.
- The following limitation applies to software upgrades from 7.0(3)I5 to 10.1(x) or 9.2(3) to 10.1(x):

  If you have the same NetFlow configuration in both VLAN and SVI, you must remove the NetFlow flow monitor from the VLAN configuration prior to the upgrade. Once upgraded, reconfigure NetFlow by creating a new flow monitor and adding it to the VLAN configuration. Failure to perform these steps results in error messages and the inability to modify the VLAN NetFlow configuration in the upgraded software.
- When upgrading from Cisco NX-OS Releases 7.0(3)I4(8), 7.0(3)I5(3), and 7.0(3)I6(1) to Cisco NX-OS Release 10.1(x) results in a disruptive upgrade. If syncing images to standby SUP failed during the disruptive upgrade from Cisco NX-OS Releases 7.0(3)I4(8), 7.0(3)I5(3,) or 7.0(3)I6(1) to 10.1(x), you should manually copy the image to the standby SUP and perform the disruptive upgrade.
- When upgrading directly to Cisco NX-OS Release 10.1(x) from any release prior to 7.0(x), the upgrade will be disruptive. For a non-disruptive upgrade, an intermediate upgrade to Cisco NX-OS Release 9.x is required. We recommend upgrading to the latest release of Cisco NX-OS Release 9.3(x) as an intermediate hop for the upgrade. For information about the supported upgrade paths, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.
- When upgrading from Cisco NX-OS Release 7.0(3)I6(1) or 7.0(3)I7(1) to Cisco NX-OS Release 10.1(x), if the Cisco Nexus 9000 Series switches are running vPC and they are connected to an IOS-based switch via Layer 2 vPC, there is a likelihood that the Layer 2 port channel on the IOS side will become error disabled. The workaround is to disable the spanning-tree etherchannel guard misconfig command on the IOS switch before starting the upgrade process.

  Once both the Cisco Nexus 9000 Series switches are upgraded, you can re-enable the command.
- If you are upgrading from Cisco NX-OS Release 7.0(3)I5(2) to Cisco NX-OS Release 10.1(x) by using the **install all** command, BIOS will not be upgraded due to CSCve24965. When the upgrade to Cisco NX-OS Release 10.1(x) is complete, use the **install all** command again to complete the BIOS upgrade, if applicable.
- An upgrade that is performed via the **install all** command for Cisco NX-OS Release 7.0(3)I2(2b) to Release 10.1(x) might result in the VLANs being unable to be added to the existing FEX HIF trunk ports. To recover from this, the following steps should be performed after all FEXs have come online and the HIFs are operationally up:

  1. Enter the copy run bootflash:fex_config_restore.cfg command at the prompt.
  2. Enter the copy bootflash:fex_config_restore.cfg running-config echo-commands command at the prompt.
- In Cisco NX-OS Release 7.0(3)I6(1) and earlier, performing an ASCII replay or running the copy file run command on a FEX HIF configuration requires manually reapplying the FEX configuration after the FEX comes back up.
- When upgrading to Cisco NX-OS Release 10.1(x) from 7.0(3)I2(x) or before and running EVPN VXLAN configuration, an intermediate upgrade to 7.0(3)I4(x) or 7.0(3)I5(x) or 7.0(3)I6(x) is required.
- Before enabling the FHS on the interface, we recommend that you carve the ifacl TCAM region on Cisco Nexus 9300 and 9500 platform switches. If you carved the ifacl TCAM region in a previous release, you

must reload the system after upgrading to Cisco NX-OS Release 10.1(x). Uploading the system creates the required match qualifiers for the FHS TCAM region, ifacl.

- Before enabling the FHS, we recommend that you carve the ing-redirect TCAM region on Cisco Nexus 9200 and 9300-EX platform switches. If you carved the ing-redirect TCAM region in a previous release, you must reload the system after upgrading to Cisco NX-OS Release 10.1(x). Uploading the system creates the required match qualifiers for the FHS TCAM region, ing-redirect.
- Upgrading from Cisco NX-OS Release 9.3(1), 9.3(2) or 9.3(3) to a higher release, with Embedded Event Manager (EEM) configurations that are saved to the running configuration, may cause a DME error to be presented. The error is in the output of the **show consistency-checker dme running-config enhanced** command, specifically, the event manager commands. If this error occurs, delete all EEM applet configurations after completing the ISSU, then reapply the EEM configurations.
- For any prior release version upgrading to Cisco NX-OS Release 9.3(5) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
  - **logging level evmc** *value*
  - **logging level mvsh** *value*
  - **logging level fs-daemon** *value*
- For any prior release version upgrading to Cisco NX-OS Release 9.3(6) using ISSU, if the following logging level commands are configured, they are missing in the upgraded version and must be reconfigured:
  - **logging level evmc** *value*
  - **logging level mvsh** *value*
- An error occurs when you try to perform an ISSU if you changed the reserved VLAN without entering the copy running-config save-config and reload commands.
- The install all command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore it is not recommended.
- Upgrading from Cisco NX-OS Release 7.0(3)I1(2), Release 7.0(3)I1(3), or Release 7.0(3)I1(3a) requires installing a patch for Cisco Nexus 9500 platform switches only. For more information on the upgrade patch, see Patch Upgrade Instructions.
- An ISSU can be performed only from a Cisco NX-OS Release 7.0(3)I4(1) to a later image.
- While performing an ISSU, VRRP and VRRPv3 displays the following messages:
  - If VRRPv3 is enabled:

```
2015 Dec 29 20:41:44 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
"vrrpv3" has sent the following message: Feature vrrpv3 is configured. User can
change
vrrpv3 timers to 120 seconds or fine tune these timers based on upgrade time on all
 Vrrp
Peers to avoid Vrrp State transitions. - sysmgr
```

  - If VRRP is enabled:

```
2015 Dec 29 20:45:10 MDP-N9K-6 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: ISSU ERROR: Service
 "vrrp-
eng" has sent the following message: Feature vrrp is configured. User can change
vrrp
timers to 120 seconds or fine tune these timers based on upgrade time on all Vrrp
Peers to
avoid Vrrp State transitions. - sysmgr
```

- Guest Shell is disabled during an ISSU and reactivated after the upgrade. Any application running in the Guest Shell is affected.
- Schedule the upgrade when your network is stable and steady.
- Avoid any power interruption, which could corrupt the software image, during the installation procedure.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software upgrade. See the Hardware Installation Guide for your specific chassis.
- Perform the installation on the active supervisor module, not the standby supervisor module.
- The **install all** command is the recommended method for software upgrades because it performs configuration compatibility checks and BIOS upgrades automatically. In contrast, changing the boot variables and reloading the device bypasses these checks and the BIOS upgrade and therefore is not recommended.

Note For Cisco Nexus 9500 platform switches with -R line cards, you must save the configuration and reload the device to upgrade from Cisco NX-OS Release 7.0(3)F3(5) to 9.3(1). To upgrade from Cisco NX-OS Release 9.2(2) or 9.2(3), we recommend that you use the **install all** command.

- You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.
- When upgrading from Cisco Nexus 94xx, 95xx, and 96xx line cards to Cisco Nexus 9732C-EX line cards and their fabric modules, upgrade the Cisco NX-OS software before inserting the line cards and fabric modules. Failure to do so can cause a diagnostic failure on the line card and no TCAM space to be allocated. You must use the **write_erase** command followed by the **reload** command.
- If you upgrade from a Cisco NX-OS release that supports the CoPP feature to a Cisco NX-OS release that supports the CoPP feature with additional classes for new protocols, you must either run the setup utility using the **setup** command or use the **copp profile** command for the new CoPP classes to be available. For more information on these commands, see the "Configuring Control Plane Policing" chapter in the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide, Release 10.1(x)* .
- For secure POAP, ensure that DHCP snooping is enabled and set firewall rules to block unintended or malicious DHCP servers. For more information on POAP, see the *Cisco Nexus 9000 Series Fundamentals Configuration Guide, Release 10.1(x)*.

- When you upgrade from an earlier release to a Cisco NX-OS release that supports switch profiles, you have the option to move some of the running-configuration commands to a switch profile. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.1(x)*.
- By default, the software upgrade process is disruptive.
- OpenFlow and LACP fast timer rate configurations are not supported for Non-Disruptive ISSU.
- Guest Shell is disabled during an ISSU and reactivated after the upgrade.
- When performing ND ISSU using BGP non-default hold timers, ensure that the BGP graceful-restart timer is reasonably long enough, for example, 180 seconds.
- During an ISSU on a Cisco Nexus 9300 Series switch, all First-Hop Redundancy Protocols (FHRPs) will cause the other peer to become active if the node undergoing the ISSU is active.
- Make sure that both vPC peers are in the same mode (regular mode or enhanced mode) before performing a non-disruptive upgrade.

Note vPC peering between an enhanced ISSU mode (boot mode lxc) configured switch and a non-enhanced ISSU mode switch is not supported.

- During an ISSU, the software reload process on the first vPC device locks its vPC peer device by using CFS messaging over the vPC communications channel. Only one device at a time is upgraded. When the first device completes its upgrade, it unlocks its peer device. The second device then performs the upgrade process, locking the first device as it does so. During the upgrade, the two vPC devices temporarily run different releases of Cisco NX-OS; however, the system functions correctly because of its backward compatibility support.
- ISSU is not supported when onePK is enabled. You can run the **show feature | include onep** command to verify that this feature is disabled before performing an ISSU or enhanced ISSU.
- In general, ISSUs are supported for the following:
  - From a major release to any associated maintenance release.
  - From the last two maintenance releases to the next two major releases.
  - From an earlier maintenance release to the next two major releases.

Note For a list of specific releases from which you can perform a disruptive upgrade or a nondisruptive ISSU, see the Cisco Nexus 9000 Series NX-OS Release Notes for your particular release.

- After performing ISSU on Cisco Nexus 9300 platform switches, you may see the MTS_OPC_CLISH message on the vPC peers. MTS_OPC_CLISH is the last MTS code that is sent from the back-end component to the VSH to specify the end of the show command output.

  If the user executes a show command that produces more output and keeps the session on for more than 3 minutes, the following warning message may be displayed on the console. As a workaround, you can

set the terminal length as 0 using the **terminal length 0** command or the **show <command> | no-more** option.

```
--More--2018 Jun 5 19:11:21 Th-agg1 %$ VDC-1 %$ Jun 5 19:11:20 %KERN-2-SYSTEM_MSG:
[12633.219113]
App vsh.bin on slot 1 vdc 1 SUP sap 64098(cli_api queue) did not drop MTS_OPC_CLISH
with
msg_id 0x675ecf from sender sap 64132(NULL) in 180 sec, contact app owner - kernel


(config)# show ip mroute detail
IP Multicast Routing Table for VRF "default"

Total number of routes: 4801
Total number of (*,G) routes: 2400
Total number of (S,G) routes: 2400
Total number of (*,G-prefix) routes: 1

(*, 225.0.0.1/32), uptime: 00:09:32, igmp(1) pim(0) ip(0)
  RPF-Source: 10.10.10.3 [11/110]
  Data Created: No
  VPC Flags
    RPF-Source Forwarder
  Stats: 15/720 [Packets/Bytes], 0.000   bps
  Stats: Inactive Flow
  Incoming interface: Ethernet1/1, RPF nbr: 12.0.0.2
  LISP dest context id: 0  Outgoing interface list: (count: 1) (bridge-only: 0)
    Vlan2001, uptime: 00:09:32, igmp (vpc-svi)


(60.60.60.2/32, 225.0.0.1/32), uptime: 00:09:31, ip(0) mrib(1) pim(0)
  RPF-Source: 60.60.60.2 [20/110]
  Data Created: Yes
  VPC Flags
--More--2018 Jun  5 19:11:21 Th-agg1 %$ VDC-1 %$ Jun  5 19:11:20 %KERN-2-SYSTEM_MSG:
[12633.219113] App vsh.bin on slot 1 vdc 1 SUP
sap 64098(cli_api queue) did not drop MTS_OPC_CLISH with msg_id 0x675ecf from sender
sap 64132(NULL) in 180 sec,
contact app owner - kernel
```

There is no functionality impact or traffic loss due to this issue. All the MTS messages are drained once the show command displays the complete output, the user enters CTRL+c, or the session gets closed.

- Occasionally, while the switch is operationally Up and running, the Device not found logs are displayed on the console. This issue is observed because the switch attempts to find an older ASIC version and the error messages for the PCI probe failure are enabled in the code. There is no functionality impact or traffic loss due to this issue.
- ISSU is not supported if EPLD is not at Cisco NX-OS Release 7.0(3)I3(1) or later.
- ISSU supports EPLD image upgrades using **install all nxos** <*nxos-image*> **epld** <*epld-image*> command, during disruptive system (NX-OS) upgrade.
- A simplified NX-OS numbering format is used for platforms that are supported in Cisco NX-OS 10.1(x) releases. In order to support a software upgrade from releases prior to Cisco NX-OS Release 7.0(3)I7(4) that have the old release format, an installer feature supplies an I9(x) label as a suffix to the actual release during the **install all** operation. This label is printed as part of the image during the install operation from any release prior to Cisco NX-OS Release 7.0(3)I7(4) to 10.1(x), and it can be ignored. See the following example.

```
switch# install all nxos bootflash:nxos.9.3.1.bin
Installer will perform compatibility check first. Please wait.
```

```
Installer is forced disruptive

Verifying image bootflash:/nxos.9.3.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.9.3.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.9.3.1.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable   Impact       Install-type  Reason
------  --------  ------------  ------------  ------
  1       yes      disruptive     reset       Incompatible image for ISSU

Images will be upgraded according to following table:
Module   Image              Running-Version(pri:alt)  New-Version         Upg-Required
------  -------  ------------------------------------ --------------------  ------------

  1      nxos                                 7.0(3)I7(3)          9.3(1)I9(1)
 yes
  1      bios     v07.61(04/06/2017):v07.61(04/06/2017)   v05.33(09/08/2018)
 yes


Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y
```

- Beginning with Cisco NX-OS Release 9.3(5), standard, nondisruptive ISSU, **on switches that are configured with uRPF**, is supported on the following:
  - Cisco Nexus 9300-EX platform switches
  - Cisco Nexus 9300-FX/FX2 platform switches
  - Cisco Nexus 9300-GX platform switches

Note Prior to Cisco NX-OS Release 9.3(5), if any of the above switches were configured with uRPF, standard, nondisruptive ISSU was not supported.

- ISSU is blocked if **boot poap enable** is configured.
- When you upgrade from Cisco NX-OS Release 7.0(3)I7(1), 7.0(3)I7(2) or 7.0(3)I7(3) to Cisco NX-OS Release 10.2(x), the upgrade fails with below error message:

```
switch(config)# install all nxos bootflash:nxos64-cs.10.2.3.F.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive
Verifying image bootflash:/nxos64-cs.10.2.3.F.bin for boot variable "nxos".
[####################] 100% -- SUCCESS
```

```
Verifying image type.
[####################] 100% -- SUCCESS
Preparing "nxos" version info using image bootflash:/nxos64-cs.10.2.3.F.bin.
[####################] 100% -- SUCCESS
Preparing "bios" version info using image bootflash:/nxos64-cs.10.2.3.F.bin.
[####################] 100% -- SUCCESS
Pre-upgrade check failed. Return code 0x40930076 (Parallel downgrade to target version
 is not supported). <<<<<
```

- Make sure that you follow below procedure to upgrade to 10.2(x) release:
  - Upgrade from 7.0(3)I7(1), 7.0(3)I7(2) or 7.0(3)I7(3) to 7.0(3)I7(5) and above code or 9.x code
  - Upgrade from 7.0(3)I7(5) or 9.x code to 10.2(x) code

- When you upgrade a Nexus 9000 switch from NX-OS Release 7.x with an attached FEX in straight-through mode to 9.x and then to 10.x, the FEX Layer 2 Host Interface (HIF) configuration can be lost after upgrading to a 10.x Release. This occurs due to a design change in handling Layer 2 FEX HIF ports at boot time from Release 9.x to 10.x.

Note The issue occurs only for FEX connected in a straight-through mode and not for dual-homed (A-A) mode.

To resolve this, run the following non-intrusive commands before upgrading the switch from 9.x to 10.x:

1. Apply **no switchport** only on all Layer 3 (L3) physical and Layer 3 (L3) port-channel interfaces. For example,

   ```
   switch(config)# interface e1/1
   switch(config-if)# no switchport
   ```

2. Configure **system default switchport** globally and save the configuration. For example,

   ```
   switch(config)# system default switchport
   switch(config)# copy r s
   ```

Note The issue does not occur if:

- the switch was originally booted in 9.x with an attached FEX and then upgraded to 10.x.
- the switch was upgraded from 7.x to 9.x without an attached FEX, and the FEX was added later in 9.x before upgrading to 10.x.

- On performing a non-disruptive ISSU from Cisco NX-OS Release 7.0(3)I6(1) to any higher version, a traffic loss might occur based on the number of VLANs configured. To avoid traffic loss, it is recommended to increase the routing protocol's graceful restart timer to higher value. The recommended value of the graceful restart timer is 600 seconds. You can further increase or decrease this value based on the scale of the configuration.
- Beginning with Cisco NX-OS Release 10.1(1), **Fs_daemon** does not support **snmpwalk** on devices with more than 5000 files. When performing snmpwalk on a device with more than 5000 files, the error **resourceUnavailable (This is likely a out-of-memory failure within the agent)** is an expected behaviour.

- Beginning with Cisco NX-OS Release 10.1(2), CoPP is supported on N9K-X9624D-R2 and N9K-C9508-FM-R2 platform switches.
- Beginning with Cisco NX-OS Release 10.1(2), RACL is supported on N9K-X9624D-R2 and N9K-C9508-FM-R2 platform switches.
- While performing an ISSU from Cisco NX-OS Release 9.3(5), 9.3(6), 9.3(7), 10.1(1), or 10.1(2) to Cisco NX-OS Release 10.2(1) or higher release, ISSU will be blocked.
- ISSU is blocked when the delay config is present in track list Boolean/weight.
- If the IPv6 ND timeouts during ISSU, then the IPv6 BFD session may flap after the ISSU.
- Beginning with Cisco NX-OS Release 10.2(3)F, non-disruptive ISSU is supported for VPC fabric peering on all Cisco Nexus 9300-X TORs. Both standard and enhanced non-disruptive upgrades are supported. Note that ISSU should be started or triggered when there is no failure. An example for failure would be one of the VPC legs is down.
- The recommended routing protocol graceful restart timer is 600 seconds and nve source-interface hold-down-time is 400 seconds.
- It is recommended to set **disable-fka** on VFC interfaces in E or F mode, when invoking ND native ISSU on switch mode testbed. If not, it can be disruptive.
- When ISSU is executed from Cisco NX-OS Release 10.2.1 or 10.2.2 to 10.2.3 or greater 10.2.x releases, BIOS upgrade is not supported for N9K-X9716D-GX, N9K-C9504-FM-G, and N9K-C9508-FM-G cards. To upgrade BIOS after ISSU is completed, use any one of the following options:
  - Execute the following commands:
    1. **install all nxos** <*image*>
    2. **install all bios-force**
  - Use the following bios force option directly: **install all nxos** <*image*> **bios-force**.
- If there is a VRF scale, for a non-disruptive ISSU under each VRF, you must configure graceful restart timer to 300 seconds.
-
- During upgrade, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, upgrade with binary restore retains the primary key after the reboot.
- Non-disruptive ISSU is not supported on interfaces with 2.5G or 5G speed on N9K-C93108TC-FX3P platform. For more information, see CSCwq38959.

Unsupported PIDs

The table displays the list of unsupported PIDs from various Cisco NX-OS Releases.

Unsupported PIDs	Cisco NX-OS Release
N9K-C93180LC-EX	9.3(x)

ISSU Platform Support

The following tables identify the platforms supporting standard and enhanced ISSU, and the release when the support was introduced.

Note Enhanced ISSU to Cisco NX-OS Release 10.1(x) is not supported as there are kernel updates that cannot take effect without reloading the underlying kernel. The system will prompt the following message:

```
Host kernel is not compatible with target image. Full ISSU will be performed and control
plane will be impacted.
```

In effect, system will perform non-disruptive ISSU instead of enhanced ISSU.

ISSU for Cisco Nexus 9200 Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with Cisco NX-OS Release 7.0(3)I6(1): Cisco Nexus 92300YC Beginning with Cisco NX-OS Release 9.3(3): Cisco Nexus 92348GC-X	Both ISSU types are disruptive for Cisco Nexus 9200 platform switches configured with the following features: • Segment routing • Tetration
Enhanced	Cisco Nexus 92300YC	

ISSU for Cisco Nexus 9300 Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with Cisco NX-OS Release 9.3(3): Cisco Nexus 9332C Cisco Nexus 9364C **Note** ISSU on Cisco Nexus 9300 platform switches is supported when the switch is the spanning tree root. You can use the **show spanning-tree issu-impact** command to verify if the switch meets this criteria.	Both ISSU types are disruptive for Cisco Nexus 9300 platform switches configured with the following features: • Dual-homed FEX • Segment routing • MACsec
Enhanced	Beginning with Cisco NX-OS Release 9.3(5): Cisco Nexus 9332C Cisco Nexus 9364C **Note** ISSU on Cisco Nexus 9300 platform switches is supported when the switch is the spanning tree root. You can use the **show spanning-tree issu-impact** command to verify if the switch meets this criteria.	

ISSU for Cisco Nexus 9300-X Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with Cisco NX-OS Release 10.2(3)F, VPC Fabric peering is supported on Cisco Nexus 9300-X TORs.	Beginning with Cisco NX-OS Release 10.2(3)F, the following VXLAN/ VPC features are not supported during non- disruptive ISSU for VPC Fabric Peering: • TRM • VXLAN IPv6 underlay • Proportional Multipath for VNF • VXLAN Flood-and-learn • HSRP and VRRP • VXLAN Cloudsec • VXLAN to SR Handoff and all Handoff features • Multi-Site • MACsec
Enhanced	Beginning with Cisco NX-OS Release 10.2(3)F, VPC Fabric peering is supported on Cisco Nexus 9300-X TORs.	

ISSU for Cisco Nexus 9300-EX Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with Cisco NX-OS Release 7.0(3)I6(1): Cisco Nexus 93108TC-EX Cisco Nexus 93180YC-EX	Both ISSU types are disruptive for Cisco Nexus 9300-EX platform switches configured with the following features: • Segment routing • Tetration • MACsec **Note** Beginning with Cisco NX-OS Release 10.2(1), both ISSU types are non-disruptive for Cisco Nexus 9300-EX platform switches configured with Straight-Through FEX and Dual-Homed FEX.
Enhanced	Beginning with Cisco NX-OS Release 7.0(3)I7(3): Cisco Nexus 93108TC-EX Cisco Nexus 93180YC-EX	

ISSU for Cisco Nexus 9300-FX Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Cisco NX-OS Release 9.3(1) and 9.3(2): None Beginning with Cisco NX-OS Release 9.3(3): Cisco Nexus 9336C-FX2 Cisco Nexus 93240YC-FX2 Cisco Nexus 93240YC-FX2Z Cisco Nexus 9348GC-FXP Cisco Nexus 93108TC-FX Cisco Nexus 93180YC-FX Beginning with Cisco NX-OS Release 10.2(1)F: Cisco Nexus 93180YC-FX3 Cisco Nexus 93180YC-FX3S	Standard ISSU is disruptive for Cisco Nexus 9300-FX platform switches configured with the following features: • Segment Routing • TRM Feature • MACsec **Note** Beginning with Cisco NX-OS Release 10.2(1), Standard ISSU is non-disruptive for Cisco Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX.

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Enhanced	Cisco NX-OS Release 9.3(1), 9.3(2), and 9.3(3): None Beginning with Cisco NX-OS Release 9.3(5): Cisco Nexus 9336C-FX2 Cisco Nexus 93240YC-FX2 Cisco Nexus 93216TC-FX2 Cisco Nexus 93360YC-FX2 Cisco Nexus 93240YC-FX2Z Cisco Nexus 9348GC-FXP Cisco Nexus 93108TC-FX Cisco Nexus 93180YC-FX Beginning with Cisco NX-OS Release 10.1(1), Enhanced ISSU is supported on the following platforms with FC/FCoE features: Cisco Nexus 93360YC-FX2 Cisco Nexus 93180YC-FX Beginning with Cisco NX-OS Release 10.2(1)F, Enhanced ISSU is supported on the following platforms: Cisco Nexus 93180YC-FX3 Cisco Nexus 93180YC-FX3S Beginning with Cisco NX-OS Release 10.2(2)F, Enhanced ISSU is supported on the following platform with FC/FCoE features: N9K-C9336C-FX2-E	Enhanced ISSU is disruptive for Cisco Nexus 9300-FX platform switches configured with the following features: • Segment Routing • TRM Feature • MACsec **Note** In Cisco NX-OS Releases 9.3(x), Enhnaced ISSU on Cisco Nexus 93360YC-FX2 and Cisco Nexus 93180YC-FX with FC/FCoE features will be disruptive. **Note** Beginning with Cisco NX-OS Release 10.2(1), Enhanced ISSU is non-disruptive for Cisco Nexus 9300-FX platform switches configured with Straight-Through FEX and Dual-Homed FEX.

ISSU for Cisco Nexus 9300-GX Platform Switches

ISSU Type	Release/Supported Platforms	Features Not Supported with Non-disruptive ISSU
Standard	Beginning with Cisco NX-OS Release 10.1(1): Cisco Nexus 9364C-GX Cisco Nexus 9316D-GX Cisco Nexus 93600CD-GX **Note** Beginning with Cisco NX-OS Release 10.3(3)F, standard ISSU is not supported on Cisco Nexus 9300-GX platform switches.	• TRM Feature • Segment Routing
Enhanced	Beginning with Cisco NX-OS Release 10.1(1): Cisco Nexus 9364C-GX Cisco Nexus 9316D-GX Cisco Nexus 93600CD-GX Beginning with Cisco NX-OS Release 10.2(2)F, Enhanced ISSU is supported on Cisco Nexus 9300-GX2B platform switches. Beginning with Cisco NX-OS Release 10.2(3)F, Enhanced ISSU is supported on Cisco Nexus 9300-GX2A platform switches.	• TRM Feature • Segment Routing

Cisco NX-OS Software Downgrade Guidelines

Before attempting to downgrade to an earlier software release, follow these guidelines:

- The only supported method of downgrading a Cisco Nexus 9000 Series switch is to utilize the install all command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.

  Disable the Guest Shell if you need to downgrade from Cisco NX-OS Release 9.3(x) to an earlier release.

  - Performing an ISSU downgrade from Cisco NX-OS Release 9.3(x) to Release 7.0(3)I4(1) with an FCoE (Fiber Channel over Ethernet) NPV (N-port Virtualization) configuration causes the port channel to crash with a core file:

    ```
    [################## ] 38%2016 Apr 18 20:52:35 n93-ns1 %$ VDC-1 %$ %SYSMGR-2-
    SERVICE_CRASHED: Service "port-channel" (PID 14976) hasn't caught signal 11 (core
    will
    be saved)
    ```

  - ISSU (non-disruptive) downgrade is not supported

- On Nexus 9500 switches with N9508-E2 Fabric module, downgrade from any 9.x or 10.x supported releases to any unsupported releases of 7.x is not supported.

- When downgrading from the Cisco NX-OS Release 9.3(x) to earlier releases, any ACL with the statistics per-entry command enabled and applied as RACL needs the statistics per-entry command removed from the running configuration before downgrading. Otherwise, the interfaces on which this ACL is applied as a RACL will be error disabled after the downgrade.
- Prior to downgrading a Cisco Nexus 9500-series switch, with -FX or -FX+EX line cards, from Cisco NX-OS Release 10.1(x) to earlier releases (9.2(x) or 7.x), the TCAM region that applies to NetFlow (ing-netflow) should be carved to zero (0) using the following command:

  hardware access-list tcam region ing-netflow 0

  The configuration change is required because the default ing-netflow TCAM region in 9.3(1) and onwards is 512 while the default in 9.2(x) and earlier is 0.
- When downgrading from the Cisco NX-OS Release 10.1(x) to a release prior to 9.3(x), make sure that the ACL TCAM usage for ingress features does exceed the allocated TCAM space in the absence of the label sharing feature. Label sharing is a new feature in Cisco NX-OS Release 9.3(x). Otherwise, interfaces with RACLs that could not fit in the TCAM will be disabled after the downgrade.
- Software downgrades should be performed using the **install all** command. Changing the boot variables, saving the configuration, and reloading the switch is not a supported method to downgrade the switch.
- The following limitation applies to Cisco Nexus platform switches that support Trust Anchor Module (TAM):

  The TACACS global key cannot be restored when downgrading from Cisco NX-OS Release 9.3(3) and higher to any earlier version. TAM was updated to version-7 in 9.3(3), but earlier NX-OS versions used TAM version-3.
- iCAM must be disabled before downgrading from Release 9.2(x) or Release 9.3(x) → 7.0(3)I7(1). Only Release 9.3(1) → Release 9.2(4) can be performed if iCAM is enabled.
- Beginning with Cisco NX-OS Release 9.3(3), new configuration commands exist for SRAPP (with sub-mode options for MPLS and SRTE). The SRAPP configuration on the switch running release 9.3(3) (or later) will not be present if the switch is downgraded to an earlier release.
- On devices with dual supervisor modules, both supervisor modules must have connections on the console ports to maintain connectivity when switchovers occur during a software downgrade. See the Hardware Installation Guide for your specific chassis.
- Cisco NX-OS automatically installs and enables the guest shell by default. However, if the device is reloaded with a Cisco NX-OS image that does not provide guest shell support, the existing guest shell is automatically removed and a %VMAN-2-INVALID_PACKAGE message is issued. As a best practice, remove the guest shell with the **guestshell destroy** command before downgrading to an earlier Cisco NX-OS image.
- You must delete the switch profile (if configured) when downgrading from a Cisco NX-OS release that supports switch profiles to a release that does not. For more information, see the *Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 10.1(x)*.
- Software downgrades are disruptive. In-service software downgrades (ISSDs), also known as nondisruptive downgrades, are not supported.
- When downgrading from Cisco NX-OS Release 9.3(3) or later to 7.0(3)I7(7), disable BFD for the BGP neighbor prefix peer using the **no bfd** command.

- While downgrading from the Cisco NX-OS Release 10.2(1)F or higher to an earlier release, the **install all** command is blocked when the delay config is present in track list Boolean/weight.
- While performing ISSD from Cisco NX-OS Release 10.2(3)F to Cisco NX-OS Release 10.2(2)F with **epbr L2** applied on interfaces, remove the policies from interfaces before performing ISSD to avoid the duplicate tracks issue.
- Beginning with Cisco NX-OS Release 10.2(3)F, if you have configured the **lldp chassis-id switch** command, then you must disable the command before performing ISSD.
- Beginning with 10.2(3)F, although application of ePBR policy to access ports is supported, downgrading with this configuration is not recommended.
- During downgrade, where both source and target images support Type-6 encryption, while performing device reload, if ASCII replay is triggered without binary restore, primary key gets lost. The primary key must be reconfigured after device reload. Use the **key config-key ascii** command to reconfigure the primary key and avoid encryption issues. However, downgrade with binary restore retains the primary key after the reboot, provided both source and target images support Type-6 encryption.

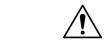
  If you downgrade the system from an image that supports Type-6 encryption to an image that does not support Type-6 encryption, compatibility check fails.

Upgrade Paths

For ISSU compatibility for all release and information about the upgrade paths, see the Cisco Nexus 9000 and 3000 Upgrade and ISSU Matrix.

Upgrade Patch Instructions

On Cisco Nexus 9500 series switches only, a software upgrade from Cisco NX-OS Release 7.0(3)I1(2), 7.0(3)I1(3), or 7.0(3)I1(3a) to any other Cisco NX-OS release requires installing two patches prior to upgrading using the **install all** command. These patches are available for each respective release and can be downloaded using the links below.



Caution Failing to follow this procedure could require console access in order to recover the switch after the upgrade.

Note These patches are only for upgrading. After the upgrade, the patch is automatically removed. If you decide not to upgrade after installing the patches, do not deactivate it. Deactivating the patch may cause a bios_daemon crash.

Cisco NX-OS Release 7.0(3)I1(2) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3) Upgrade Patch

Cisco NX-OS Release 7.0(3)I1(3a) Upgrade Patch

To install these patches prior to upgrading using the install all command, follow the instructions shown below. An example is demonstrated below with an NX-OS software patch and upgrade from 7.0(3)I1(2) to 7.0(3)I7(1):

1. Add both patches with the **install add bootflash:**{*patch-file.bin*} command.

```
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 16 completed successfully at Thu Mar  3 04:24:13 2016
switch(config)# install add bootflash:n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 17 completed successfully at Thu Mar  3 04:24:43 2016
```

2. Activate both patches with the **install activate** {*patch-file.bin*} command.

```
switch(config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 18 completed successfully at Thu Mar  3 04:28:38 2016
switch (config)# install activate n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 19 completed successfully at Thu Mar  3 04:29:08 2016
```

3. Commit both patches with the **install commit** {*patch-file.bin*} command.

```
switch(config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16604.bin
Install operation 20 completed successfully at Thu Mar  3 04:30:38 2016
switch (config)# install commit n9000-dk9.7.0.3.I1.2.CSCuy16606.bin
Install operation 21 completed successfully at Thu Mar  3 04:31:16 2016
```

4. Proceed with an NX-OS software upgrade to the desired target release with the **install all** command.

```
switch (config)# install all nxos bootflash:nxos.7.0.3.I7.1.bin
Installer will perform compatibility check first. Please wait.
uri is: /nxos.7.0.3.I7.1.bin
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I7.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
```

```
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Preparing "lcn9k" version info using image bootflash:/nxos.7.0.3.I7.1.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS

Compatibility check is done:
Module  bootable          Impact  Install-type  Reason
------  --------  --------------  ------------  ------
     1       yes      disruptive         reset  Incompatible image
     6       yes      disruptive         reset  Incompatible image
     8       yes      disruptive         reset  Incompatible image
     9       yes      disruptive         reset  Incompatible image
    10       yes      disruptive         reset  Incompatible image
    11       yes      disruptive         reset  Incompatible image
    14       yes      disruptive         reset  Incompatible image
    15       yes      disruptive         reset  Incompatible image
    16       yes      disruptive         reset  Incompatible image
    21       yes      disruptive         reset  Incompatible image
    22       yes      disruptive         reset  Incompatible image
    23       yes      disruptive         reset  Incompatible image
    24       yes      disruptive         reset  Incompatible image
    25       yes      disruptive         reset  Incompatible image
    26       yes      disruptive         reset  Incompatible image
    27       yes      disruptive         reset  Incompatible image
    28       yes      disruptive         reset  Incompatible image
    29       yes      disruptive         reset  Incompatible image
    30       yes      disruptive         reset  Incompatible image

Images will be upgraded according to following table:
Module  Image               Running-Version(pri:alt)         New-Version  Upg-Required
------  -----  -------------------------------------  ------------------  ------------
     1  lcn9k                             7.0(3)I1(2)         7.0(3)I7(1)           yes
     1   bios                     v01.42(00:v01.42(00           v01.48(00           yes
     6  lcn9k                             7.0(3)I1(2)         7.0(3)I7(1)           yes
```

```
     6   bios                     v01.48(00:v01.48(00           v01.48(00            no
     8  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
     8   bios                     v01.48(00:v01.29(00           v01.48(00            no
     9  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
     9   bios                     v01.48(00:v01.35(00           v01.48(00            no
    10  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    10   bios                     v01.48(00:v01.42(00           v01.48(00            no
    11  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    11   bios                     v01.48(00:v01.52(00           v01.48(00            no
    14  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    14   bios                     v01.48(00:v01.48(00           v01.48(00            no
    15  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    15   bios                     v01.48(00:v01.40(00           v01.48(00            no
    16  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    16   bios                     v01.48(00:v01.42(00           v01.48(00            no
    21  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    21   bios                     v01.48(00:v01.42(00           v01.48(00            no
    22  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    22   bios                     v01.48(00:v01.40(00           v01.48(00            no
    23  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    23   bios                     v01.48(00:v01.40(00           v01.48(00            no
    24  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    24   bios                     v01.48(00:v01.40(00           v01.48(00            no
    25  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    25   bios                     v01.48(00:v01.40(00           v01.48(00            no
    26  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    26   bios                     v01.48(00:v01.40(00           v01.48(00            no
    27   nxos                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    27   bios  v08.06(09/10/2014):v08.18(08/11/2015)  v08.26(01/12/2016)           yes
    28   nxos                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    28   bios  v08.06(09/10/2014):v08.26(01/12/2016)  v08.26(01/12/2016)           yes
    29  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    29   bios                     v01.48(00:v01.35(00           v01.48(00            no
    30  lcn9k                            7.0(3)I1(2)         7.0(3)I7(1)           yes
    30   bios                     v01.48(00:v01.35(00           v01.48(00            no

Switch will be reloaded for disruptive upgrade.
Do you want to continue with the installation (y/n)?  [n] y

Install is in progress, please wait.

Performing runtime checks.
[####################] 100% -- SUCCESS

Syncing image bootflash:/nxos.7.0.3.I7.1.bin to standby.
[####################] 100% -- SUCCESS

Setting boot variables.
[####################] 100% -- SUCCESS

Performing configuration copy.
[####################] 100% -- SUCCESS

Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 6: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 8: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS
```

```
Module 9: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 10: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 11: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 14: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 15: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 16: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 21: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 22: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 23: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 24: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 25: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 26: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 27: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 28: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 29: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS

Module 30: Refreshing compact flash and upgrading bios/loader/bootrom.
Warning: please do not remove or power off the module at this time.
[####################] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.
switch(config)#
User Access Verification

switch login:
[ 2644.917727] [1456980048]  writing reset reason 88,

CISCO SWITCH Ver 8.26

CISCO SWITCH Ver 8.26
Memory Size (Bytes): 0x0000000080000000 + 0x0000000380000000
 Relocated to memory
Time: 6/3/2016  4:41:8
Detected CISCO IOFPGA
Booting from Primary Bios
Code Signing Results: 0x0
Using Upgrade FPGA
FPGA Revision        : 0x27
FPGA ID             : 0x1168153
FPGA Date           : 0x20160111
Reset Cause Register: 0x22
Boot Ctrl Register  : 0x60ff
EventLog  Register1 : 0x2000000
EventLog  Register2 : 0xfbe77fff
Version 2.16.1240. Copyright (C) 2013 American Megatrends, Inc.
Board type  1
IOFPGA @ 0xe8000000
SLOT_ID @ 0x1b
Standalone chassis
check_bootmode: grub: Continue grub
Trying to read config file /boot/grub/menu.lst.local from (hd0,4)
 Filesystem type is ext2fs, partition type 0x83

Booting bootflash:/nxos.7.0.3.I7.1.bin ...
Booting bootflash:/nxos.7.0.3.I7.1.bin
Trying diskboot
 Filesystem type is ext2fs, partition type 0x83
IOFPGA ID: 1168153
Image valid


Image Signature verification was Successful.

Boot Time: 3/3/2016  4:41:44
INIT: version 2.88 booting
Unsquashing rootfs ...

Loading IGB driver ...
Installing SSE module ... done
Creating the sse device node ... done
Loading I2C driver ...
Installing CCTRL driver for card_type 3 ...
CCTRL driver for card_index 21000 ...
old data: 4000004 new data: 1
Not Micron SSD...

Checking all filesystems.......
Installing default sprom values ...
 done.Configuring network ...
Installing LC netdev ...
Installing psdev ...
Installing veobc ...
Installing OBFL driver ...
mounting plog for N9k!
```

```
tune2fs 1.42.1 (17-Feb-2012)
Setting reserved blocks percentage to 0% (0 blocks)
Starting portmap daemon...
creating NFS state directory: done
starting 8 nfsd kernel threads: done
starting mountd: done
starting statd: done
Saving image for img-sync ...
Loading system software
Installing local RPMS
Patch Repository Setup completed successfully
dealing with default shell..
file /proc/cmdline found, look for shell
unset shelltype, nothing to do..
user add file found..edit it
Uncompressing system image: Thu Jun 3 04:42:11 UTC 2016
blogger: nothing to do.

..done Thu Mar 3 04:42:11 UTC 2016
Creating /dev/mcelog
Starting mcelog daemon
Overwriting dme stub lib
Replaced dme stub lib
INIT: Entering runlevel: 3
Running S93thirdparty-script...

2016 Mar  3 04:42:37 switch%$ VDC-1 %$  %USER-2-SYSTEM_MSG: <<%USBHSD-2-MOUNT>> logflash:
 online  - usbhsd
2016 Mar  3 04:42:37 switch%$ VDC-1 %$ Mar  3 04:42:37 %KERN-2-SYSTEM_MSG: [   12.509615]
 hwport mode=6 - kernel
2016 Mar  3 04:42:40 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Installing virtual service
 'guestshell+'
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG:
<<%ASCII-CFG-2-CONF_CONTROL>> Binary restore - ascii-cfg[13904]
2016 Mar  3 04:42:40 switch%$ VDC-1 %$  %DAEMON-2-SYSTEM_MSG:
<<%ASCII-CFG-2-CONF_CONTROL>> Restore DME database - ascii-cfg[13904]
2016 Mar  3 04:42:42 switch%$ VDC-1 %$ netstack: Registration with cli server complete
2016 Mar  3 04:43:00 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: ssnmgr_app_init called on
ssnmgr up - aclmgr
2016 Mar  3 04:43:09 switch%$ VDC-1 %$ %USER-0-SYSTEM_MSG: end of default policer - copp
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-INSTALL_STATE: Install success virtual
service 'guestshell+'; Activating
2016 Mar  3 04:43:10 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Activating virtual
service 'guestshell+'
2016 Mar  3 04:43:13 switch%$ VDC-1 %$ %CARDCLIENT-2-FPGA_BOOT_PRIMARY: IOFPGA booted
from Primary
2016 Mar  3 04:43:18 switch%$ VDC-1 %$ %USER-2-SYSTEM_MSG: IPV6 Netlink thread init
successful  - icmpv6
2016 Mar  3 04:43:19 switch%$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online


User Access Verification
switchlogin:
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 1
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 6
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 8
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 9
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 10
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
```

```
of Module 11
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 14
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 15
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 16
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 21
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 22
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 23
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 24
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 25
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 26
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 28
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 29
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PRESENT: Detected the presence
of Module 30
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 1 ok (Serial
number XYZ284014RR)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 1 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 2 ok (Serial
number XYZ285111TC)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 2 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 3 ok (Serial
number XYZ285111QQ)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 3 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 4 ok (Serial
number XYZ284014TI)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 4 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_OK: Power supply 5 ok (Serial
number XYZ284014TS)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-PS_FANOK: Fan in Power supply 5 ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 1
(Fan1(sys_fan1) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 2
(Fan2(sys_fan2) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-FANMOD_FAN_OK: Fan module 3
(Fan3(sys_fan3) fan) ok
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 30 detected (Serial
 number ABC1234DE56) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 30 powered up (Serial
 number ABC1234DE56)
2016 Mar  3 04:43:52 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 28 detected (Serial
 number :unavailable) Module-Type Supervisor Module Model :unavailable
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 29 detected (Serial
 number ABC1234DEFG) Module-Type System Controller Model N9K-SC-A
2016 Mar  3 04:43:58 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 29 powered up (Serial
 number ABC1234DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 21 detected (Serial
 number ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 22 detected (Serial
 number ABC1211DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 21 powered up (Serial
 number ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 22 powered up (Serial
 number ABC1211DEFG)
```

```
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 23 detected (Serial
 number ABC1234D5EF) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 23 powered up (Serial
 number ABC1234D5EF)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 24 detected (Serial
 number ABC1211DE3F) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 24 powered up (Serial
 number ABC1211DE3F)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 25 detected (Serial
 number ABC1213DEFG) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 25 powered up (Serial
 number ABC1213DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 26 detected (Serial
 number ABC1211DE34) Module-Type Fabric Module Model N9K-C9516-FM
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 26 powered up (Serial
 number ABC1211DE34)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 1. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 1 detected (Serial
 number ABC1217DEFG) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 1 powered up (Serial
 number ABC1217DEFG)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 9. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 9 detected (Serial
 number ABC1236D4E5) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 9 powered up (Serial
 number ABC1236D4E5)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 10. Ejector based shutdown enabled
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 10 detected (Serial
 number ABC1217EFGH) Module-Type 32p 40G Ethernet Module Model N9K-X9432PQ
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 10 powered up (Serial
 number ABC1217EFGH)
2016 Mar  3 04:44:01 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 11. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 11 detected (Serial
 number ABC123DEF4) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 11 powered up (Serial
 number ABC123DEF4)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 15. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 15 detected (Serial
 number ABC1212DEFG) Module-Type 36p 40G Ethernet Module Model N9K-X9536PQ
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 15 powered up (Serial
 number ABC1212DEFG)
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 16. Ejector based shutdown enabled
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 16 detected (Serial
 number ABCD1235DEFG) Module-Type 48x1/10G SFP+ 4x40G Ethernet Module Model N9K-X9464PX
2016 Mar  3 04:44:02 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 16 powered up (Serial
 number ABCD1235DEFG)
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 14. Ejector based shutdown enabled
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 14 detected (Serial
 number ABC9876DE5F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:08 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 14 powered up (Serial
 number ABC9876DE5F)
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 6. Ejector based shutdown enabled
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 6 detected (Serial
 number ABC9876DE3F) Module-Type 8p 100G Ethernet Module Model N9K-X9408PC-CFP2
2016 Mar  3 04:44:09 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 6 powered up (Serial
 number ABC9876DE3F)
```

```
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MODULE_EJECTOR_POLICY_ENABLED: All
Ejectors closed for module 8. Ejector based shutdown enabled
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_DETECT: Module 8 detected (Serial
 number ABC3456D7E8) Module-Type 48x1/10G-T 4x40G Ethernet Module Model N9K-X9564TX
2016 Mar  3 04:44:10 switch%$ VDC-1 %$ %PLATFORM-2-MOD_PWRUP: Module 8 powered up (Serial
 number ABC3456D7E8)
2016 Mar  3 04:44:56 switch%$ VDC-1 %$ %USBHSD-STANDBY-2-MOUNT: logflash: online
2016 Mar  3 04:47:31 switch%$ VDC-1 %$ %ASCII-CFG-2-CONF_CONTROL: System ready
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-ACTIVATION_STATE: Successfully activated
 virtual service 'guestshell+'
2016 Mar  3 04:47:51 switch%$ VDC-1 %$ %VMAN-2-GUESTSHELL_ENABLED: The guest shell has
been enabled. The command 'guestshell' may be used to access it, 'guestshell destroy'
to remove it.

User Access Verification

switch#  show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2016, Cisco and/or its affiliates.
All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under their own
licenses, such as open source.  This software is provided "as is," and unless
otherwise stated, there is no warranty, express or implied, including but not
limited to warranties of merchantability and fitness for a particular purpose.
Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or
GNU General Public License (GPL) version 3.0  or the GNU
Lesser General Public License (LGPL) Version 2.1 or
Lesser General Public License (LGPL) Version 2.0.
A copy of each such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://opensource.org/licenses/gpl-3.0.html and
http://www.opensource.org/licenses/lgpl-2.1.php and
http://www.gnu.org/licenses/old-licenses/library.txt.

Software
  BIOS: version 08.26
  NXOS: version 7.0(3)I7(1)
  BIOS compile time:  06/12/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I7.1.bin
  NXOS compile time:  2/8/2016 20:00:00 [02/09/2016 05:18:17]


Hardware
  cisco Nexus9000 C9516 (16 Slot) Chassis ("Supervisor Module")
  Intel(R) Xeon(R) CPU E5-2403 0 @ 1.80GHz with 16401664 kB of memory.
  Processor Board ID SAL1745FTPW

  Device name: switch
  bootflash:   20971520 kB
Kernel uptime is 0 day(s), 0 hour(s), 8 minute(s), 13 second(s)

Last reset at 235176 usecs after  Thu Mar  3 04:40:48 2016

  Reason: Reset due to upgrade
  System version: 7.0(3)I1(2)
  Service:

plugin
  Core Plugin, Ethernet Plugin
```

```
Active Package(s):
switch#
```

Configuring Enhanced ISSU

You can enable or disable enhanced (LXC) ISSU.

Note

- Enhanced ISSU to Cisco NX-OS Release 10.1(x) is not supported as there are kernel updates that cannot take effect without reloading the underlying kernel. The system will prompt the following message:

  ```
  Host kernel is not compatible with target image. Full ISSU will be performed and control
   plane will be impacted.
  ```

  In effect, system will perform nondisruptive ISSU instead of enhanced ISSU.

- For Cisco N9K-C9332D-GX2B [from Cisco NX-OS Release 10.2(2)F)], and N9K-C9348D-GX2A and N9K-C9364D-GX2A [from Cisco NX-OS Release 10.2(3)F] platform switches, enhanced (LXC) ISSU is the default mode, so you cannot enable or disable this mode. Also, for these switches, `virtual supervisor module` is shown in the output of the **show module** command.
- It is recommended to set **disable-fka** on the FCF, when invoking Fallback ND LXC ISSU on the NPV from Cisco NX-OS Release 10.2(3)F and higher versions. If not, it will be disruptive. Verify the output of the **show fcoe-npv issu-impact** command to know whether the **disable-fka** must be set.

Before you begin

Before you enable the LXC mode, ensure that the installed licenses do not include the 27000 string in the license file.

SUMMARY STEPS

1. **configure terminal**
2. [**no**] **boot mode lxc**
3. (Optional) **show boot mode**
4. **copy running-config startup-config**
5. **reload**

DETAILED STEPS

Procedure

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config#)`
		Enters global configuration mode.

	Command or Action	Purpose

Step 2	[**no**] **boot mode lxc**
	Example:
	`switch(config)# boot mode lxc`
	`Using LXC boot mode`
	Example:
	`switch(config)# no boot mode lxc`
	`Using normal native boot mode`
		Enables or disables enhanced (LXC) ISSU.
		Note
		In order to perform a nondisruptive enhanced ISSU, you must first boot the switch in LXC mode.

Step 3	(Optional) **show boot mode**
	Example:
	`switch(config)# show boot mode`
	`LXC boot mode is enabled`
	Example:
	`switch(config)# show boot mode`
	`LXC boot mode is disabled`
		Shows whether enhanced (LXC) ISSU is enabled or disabled.

Step 4	**copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	Saves the running configuration to the startup configuration.

Step 5	**reload**
	Example:
	`switch(config)# reload`
	`This command will reboot the system. (y/n)?  [n]`
	`Y`
	`loader>`
		Reloads the device. When prompted, press **Y** to confirm the reboot.

What to do next

Follow the instructions in Upgrading the Cisco NX-OS Software section. Make sure to choose the **non-disruptive** option if you want to perform an enhanced or regular ISSU.

Upgrading the Cisco NX-OS Software

Use this procedure to upgrade to a Cisco NX-OS 10.2(x) release.

Note Beginning with Cisco NX-OS Release 10.1(1), the Cisco Nexus -GX series platforms use the 64-bit Cisco NX-OS image file, which has the image filename that begins with "nxos64" (for example, nxos64.10.1.1.bin). The 64-bit software image, which supports software scalability, is available for the Cisco Nexus C9316D-GX, C93600CD-GX, C9364C-GX switches. The non-GX series platforms use the 32-bit Cisco NX-OS image file, which has the image filename that begins with "nxos" (for example, nxos.10.1.1.bin).

Note For Cisco Nexus 9500 platform switches with -R line cards, you must save the configuration and reload the device to upgrade from Cisco NX-OS Release 7.0(3)F3(5) to 10.1(1). To upgrade from Cisco NX-OS Release 9.2(2) or later, we recommend that you use the **install all** command.

Note If an error message appears during the upgrade, the upgrade will fail because of the reason indicated. See the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.1(x)* for a list of possible causes and solutions.

Before you begin

Before performing a nondisruptive ISSU to Cisco NX-OS Release 10.1(1), you must configure the BGP graceful restart timer to 180 seconds for Cisco Nexus 3132Q-V platform switches.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Ensure that the required space is available for the image file to be copied.
4. If you need more space on the active supervisor module, delete unnecessary files to make space available.
5. Verify that there is space available on the standby supervisor module.
6. If you need more space on the standby supervisor module, delete any unnecessary files to make space available.
7. Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
8. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
9. You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.
10. You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.
11. Check the impact of upgrading the software before actually performing the upgrade.
12. Save the running configuration to the startup configuration.
13. If required, upgrade the EPLD image using the **install all nxos <nxos-image> epld <epld-image>** command.

14. Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **non-disruptive** | **non-interruptive** | **serial**] command.
15. (Optional) Display the entire upgrade process.
16. (Optional) Log in and verify that the device is running the required software version.
17. (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

DETAILED STEPS

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this upgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Ensure that the required space is available for the image file to be copied.

```
switch# dir bootflash:
16384    Oct 30 17:05:32 2020  lost+found/
1964291584    Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-local
 4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

Note
We recommend that you have the image file for at least one previous release of the Cisco NX-OS software on the device to use if the new image file does not load successfully.

Step 4 If you need more space on the active supervisor module, delete unnecessary files to make space available.

```
switch# delete bootflash:nxos.9.2.1.bin
```

Step 5 Verify that there is space available on the standby supervisor module.

```
switch# dir bootflash://sup-standby/
16384    Oct 30 17:05:32 2020  lost+found/
1964291584    Dec 08 19:44:33 2020  nxos.10.1.1.bin
...
Usage for bootflash://sup-standby
4825743360 bytes used
16312102912 bytes free
21137846272 bytes total
```

Step 6 If you need more space on the standby supervisor module, delete any unnecessary files to make space available.

```
switch# delete bootflash://sup-standby/nxos.9.2.1.bin
```

Step 7 Log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Step 8 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# copy scp://user@scpserver.cisco.com//download/nxos64.10.2.1.F.bin
bootflash:nxos64.10.2.1.F.bin
```

Note
The compaction feature is deprecated from Cisco NX-OS Release

For software images requiring compaction, you must use SCP, HTTP, or HTTPS as the source and bootflash or USB as the destination. The following example uses SCP and bootflash:

```
switch# copy scp://user@scpserver.cisco.com//download/nxos64.10.2.1.F.bin
bootflash:nxos64.10.2.1.F.bin compact vrf management use-kstack

user1@10.65.42.196's password:
nxos64.10.2.1.F.bin 100% 1887MB 6.6MB/s 04:47
Copy complete, now saving to disk (please wait)...
Copy complete.
```

The **compact** keyword compacts the NX-OS image before copying the file to the supervisor module.

Note
Software image compaction is only supported on SCP, HTTP, or HTTPS. If you attempt compaction with any other protocol, the system returns the following error:

```
Compact option is allowed only with source as scp/http/https and destination
as bootflash or usb
```

Note
Compacted images are not supported with LXC boot mode.

Note
Software image compaction is only supported on Cisco Nexus 9300-series platform switches.

Step 9 You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.

```
switch# show file bootflash:nxos.10.1.1.bin md5sum
2242a7f876f1304118fd175c66f69b34

switch# show file bootflash:nxos.10.1.1.bin sha512sum
7f25cce57ca137a79211fb3835338aae64acf9b021b75cec5d4156e873b4274ca4f98e9a74fe4c8961f5ace99ed65f3826650599369f84ab07265d7c5d61b57f
```

Step 10 You can detect an incomplete or corrupt NX-OS software image prior to performing an upgrade by verifying the MD5, SHA256 or SHA512 checksum of the software image. To verify the MD5 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**md5sum** command and compare the resulting value to the published MD5 checksum for the software image on Cisco's Software Download website. To verify the SHA512 checksum of the software image, run the **show file bootflash:**<*IMAGE-NAME*>**sha512sum** command and compare the resulting value to the published SHA512 checksum for the software image on Cisco's Software Download website.

```
switch# show file bootflash:nxos64.10.2.1.F.bin md5sum
c49660952215822afd30bb7958a0765a

switch# show file bootflash:nxos64.10.2.1.F.bin sha256sum
2a64efbb381fabbb52054af74cf3efda1691772a49a70ddd35550431cadecf8e
```

```
switch# show file bootflash:nxos64.10.2.1.F.bin sha512sum
3bf6a771aa4a192a8e1383e348b26bb483356a9774d74ba39edbf7718248483b3391942d8103de8104deea8fda212266e70bd736220cff34943bd8e359432975
```

Step 11 Check the impact of upgrading the software before actually performing the upgrade.

```
switch# # show install all impact nxos bootflash:nxos64.10.2.1.F.bin
```

During the compatibility check, the following ISSU-related messages may appear in the Reason field:

Reason Field Message	Description
Incompatible image for ISSU	The Cisco NX-OS image to which you are attempting to upgrade does not support ISSU.
Default upgrade is not hitless	By default, the software upgrade process is disruptive. You must configure the **non-disruptive** option to perform an ISSU.

Step 12 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 13 If required, upgrade the EPLD image using the **install all nxos <nxos-image> epld <epld-image>** command.

The following is an example output of the **install all nxos <nxos-image> epld <epld-image>** command:

```
switch# install all nxos nxos.10.1.1.bin epld n9000-epld.10.1.1.img

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.10.1.1.bin for boot variable "nxos".
[####################] 100% -- SUCCESS

Verifying EPLD image bootflash:/ n9000-epld.10.1.1.img.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.10.1.1.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.10.1.1.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS


switch# install all nxos nxos.10.1.1.IJD9.0.59.bin epld n9000-epld.10.2.1.F.img

Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.10.1.1.IJD9.0.59.bin for boot variable "nxos".
[####################] 100% -- SUCCESS
```

```
Verifying EPLD image bootflash:/ n9000-epld.10.2.1.F.img.
[####################] 100% -- SUCCESS

Verifying image type.
[####################] 100% -- SUCCESS

Preparing "nxos" version info using image bootflash:/nxos.10.1.1.IJD9.0.59.bin.
[####################] 100% -- SUCCESS

Preparing "bios" version info using image bootflash:/nxos.10.1.1.IJD9.0.59.bin.
[####################] 100% -- SUCCESS

Performing module support checks.
[####################] 100% -- SUCCESS

Notifying services about system upgrade.
[####################] 100% -- SUCCESS
```

Step 14 Upgrade the Cisco NX-OS software using the **install all nxos bootflash:***filename* [**no-reload** | **non-disruptive** | **non-interruptive** | **serial**] command.

```
switch# install all nxos bootflash:nxos64.10.2.1.F.bin
```

The following options are available:

- **no-reload**—Exits the software upgrade process before the device reloads.

  Note
  When you use **install all** with **no-reload** option, no additional configuration changes can be made before you reload the device. Saving configuration in this state can result in incorrect startup configuration once you reload the device with the new version of NX-OS.

- **non-disruptive**—Performs an in-service software upgrade (ISSU) to prevent the disruption of data traffic. (By default, the software upgrade process is disruptive.)
- **non-interruptive**—Upgrades the software without any prompts. This option skips all error and sanity checks.
- **serial**—Upgrades the I/O modules in Cisco Nexus 9500 Series switches one at a time. (By default, the I/O modules are upgraded in parallel, which reduces the overall upgrade time. Specifically, the I/O modules are upgraded in parallel in this order: the first half of the line cards and fabric modules, the second half of the line cards and fabric modules, the first system controller, the second system controller.)

Note
- If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NX-OS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image, if necessary.

Step 15 (Optional) Display the entire upgrade process.

```
switch# show install all status
```

Step 16 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Step 17 (Optional) If necessary, install any licenses to ensure that the required features are available on the device. See the Cisco NX-OS Licensing Guide.

Upgrade Process for vPCs

Upgrade Process for a vPC Topology on the Primary Switch

The following list summarizes the upgrade process on a switch in a vPC topology that holds either the Primary or Operational Primary vPC roles. Steps that differ from a switch upgrade in a non-vPC topology are in bold.

Note In vPC topologies, the two peer switches must be upgraded individually. An upgrade on one peer switch does not automatically update the vPC peer switch.

In a dual-homed non-vPC access network (either a triangle or Y shaped access network), with or without STP configured, with BFD enabled and with HSRP configured on the SVIs and with HSRP configured as BFD client, transient traffic may drop for both IPv4 native unicast and/or labeled traffic after performing an ND-ISSU n fallback mode.

To counter this, configure in all the HSRP IPv4 groups for all the HSRP enabled SVIs the **timer 2 120** on both HSRP peers prior to performing the ND-ISSU. The configuration of the **timer 3 120** may lead to traffic loss.

1. **The install all command issued on the vPC primary switch triggers the installation upgrade.**
2. The compatibility checks display the impact of the upgrade.
3. The installation proceeds or not based on the upgrade impact.
4. **The configuration is locked on both vPC peer switches.**
5. The current state is saved.
6. The system unloads and runs the new image.
7. The stateful restart of the system software and application occurs.
8. The installer resumes with the new image.
9. The installation is complete.

When the installation is complete, the vPC primary switch is upgraded.

Note The vPC primary switch is running the upgraded version, and the vPC secondary switch is running the original software version.

Upgrade Process for a vPC Topology on the Secondary Switch

The following list summarizes the upgrade process on a switch in a vPC topology that holds either the Secondary or Operational Secondary vPC roles. Steps that differ from a switch upgrade in a non-vPC topology are in bold.

1. **The install all command issued on the vPC secondary switch triggers the installation upgrade.**
2. The compatibility checks display the impact of the upgrade.
3. The installation proceeds or not based on the upgrade impact.
4. The current state is saved.
5. The system unloads and runs the new image.
6. The stateful restart of the system software and application occurs.
7. The installer resumes with the new image.
8. **The configuration is unlocked on the primary and secondary switches.**
9. The installation is complete.

Downgrading to an Earlier Software Release

Note If an error message appears during the downgrade, the downgrade will fail because of the reason indicated. See the *Cisco Nexus 9000 Series NX-OS Troubleshooting Guide, Release 10.2(x)* for a list of possible causes and solutions.

SUMMARY STEPS

1. **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.
2. Log in to the device on the console port connection.
3. Verify that the image file for the downgrade is present on the active supervisor module bootflash:.
4. If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.
5. Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.
6. Check for any software incompatibilities.
7. Disable any features that are incompatible with the downgrade image.
8. Check for any hardware incompatibilities.
9. Power off any unsupported modules.
10. Save the running configuration to the startup configuration.
11. Downgrade the Cisco NX-OS software using the **install all nxos bootflash** <*nxos_image_to_downgrade*> command.

12. (Optional) Display the entire downgrade process.
13. (Optional) Log in and verify that the device is running the required software version.

DETAILED STEPS

Procedure

Step 1 **Read the release notes for the software image file for any exceptions to this downgrade procedure.** See the Cisco Nexus 9000 Series NX-OS Release Notes.

Step 2 Log in to the device on the console port connection.

Step 3 Verify that the image file for the downgrade is present on the active supervisor module bootflash:.

```
switch# dir bootflash:
```

Step 4 If the software image file is not present, log in to Cisco.com, choose the software image file for your device from the following URL, and download it to a file server: http://software.cisco.com/download/navigator.html.

Note
If you need more space on the active or standby supervisor module bootflash:, use the **delete** command to remove unnecessary files.

Step 5 Copy the software image to the active supervisor module using a transfer protocol. You can use FTP, TFTP, SCP, or SFTP.

```
switch# switch# copy scp://user@scpserver.cisco.com//download/nxos.9.2.1.bin
bootflash:nxos.9.2.1.bin
```

Step 6 Check for any software incompatibilities.

```
switch# show incompatibility-all nxos bootflash:nxos.9.2.1.bin
Checking incompatible configuration(s)
No incompatible configurations
```

The resulting output displays any incompatibilities and remedies.

Step 7 Disable any features that are incompatible with the downgrade image.

Step 8 Check for any hardware incompatibilities.

```
switch# show install all impact nxos bootflash:nxos.9.2.1.bin
```

Step 9 Power off any unsupported modules.

```
switch# poweroff module module-number
```

Step 10 Save the running configuration to the startup configuration.

```
switch# copy running-config startup-config
```

Step 11 Downgrade the Cisco NX-OS software using the **install all nxos bootflash** <*nxos_image_to_downgrade*> command.

Note

If you enter the **install all** command without specifying a filename, the command performs a compatibility check, notifies you of the modules that will be upgraded, and confirms that you want to continue with the installation. If you choose to proceed, it installs the NXOS software image that is currently running on the switch and upgrades the BIOS of various modules from the running image if required.

Step 12 (Optional) Display the entire downgrade process.

Example:

```
switch# show install all status
```

Step 13 (Optional) Log in and verify that the device is running the required software version.

```
switch# show version
```

Cisco NX-OS Upgrade History

During the life of a Cisco Nexus 9000 switch, many upgrade procedures can be performed. Upgrades can occur for maintenance purposes or to update the operating system to obtain new features. Over time, switches may be updated on numerous occasions. Viewing the types of upgrades and when they occurred can help in troubleshooting issues or simply understanding the history of the switch.

Beginning with Cisco NX-OS Release 9.3(5), Cisco Nexus 9000 switches log all upgrade activity performed over time providing a comprehensive history of these events. The stored upgrade history types are:

- Cisco NX-OS System Upgrades
- Electronic Programmable Logic Device (EPLD) Upgrades
- Software Maintenance Upgrade (SMU) Installations

View the Cisco NX-OS upgrade history by entering the **show upgrade history** command. The output displays any upgrade activity that previously occurred on the switch and defines the start and end times for each event. The following is an example output of the **show upgrade history** command:

```
switch# show upgrade history
TYPE                VERSION   DATE                    STATUS
NXOS EPLD           n9000-    26 Apr 2020 11:37:16    EPLD Upgrade completed
                    epld.9.3.4.img
NXOS EPLD           n9000-    26 Apr 2020 11:32:41    EPLD Upgrade started
                    epld.9.3.4.img
NXOS system image   9.3(5)    24 Mar 2020 20:09:10    Installation End
NXOS system image   9.3(5)    24 Mar 2020 20:05:29    Installation started
NXOS SMU            9.3(5)    03 Mar 2020 23:34:15    Patch activation ended for
                                                      nxos.libnbproxycli_patch-n9k_
                                                      ALL-1.0.0-9.3.5.lib32_n9000.rpm
NXOS SMU            9.3(5)    03 Mar 2020 23:34:03    Patch activation started for
                                                      nxos.libnbproxycli_patch-n9k_
                                                      ALL-1.0.0-9.3.5.lib32_n9000.rpm
```

Beginning with Cisco NX-OS Release 10.2(3)F, Cisco Nexus 9000 switches support new cli "**show upgrade history details**" which displays login details (user name/session ID).

View the Cisco NX-OS upgrade history details by entering the **show upgrade history details** command. The output displays user login details (user name/session ID) under LOGIN column on the switch along with upgrade history. The following is an example output of the **show upgrade history details** command:

```
switch# sh upgrade history details
     TYPE          VERSION                                  DATE                  LOGIN
                       STATUS
NXOS system image  10.2(3)                  21 Jan 2022 10:01:06     admin/10.30.216.212
       Installation End
NXOS system image  10.2(3)                  21 Jan 2022 10:00:53     admin/10.30.216.212
       Installation started
NXOS system image  10.2(3)                  21 Jan 2022 01:03:52     admin/10.30.216.212
       Installation End
```